Fermilab Service CA Certificate Policy
and Certification Practices Statement

8 August 2003

1. INTRODUCTION

1.1. Overview

This document follows the structure suggested in RFC 2527.

The public key infrastructure of Fermilab comprises three certificate authorities: the KCA, the Service CA and the Top-Level CA. This document specifies the policies and practices under which the Service CA is operated.

1.2. Identification

Document title
Fermilab Service CA Certificate Policy and Certification Practices Statement

Document version
Revision: 1.3

Document date
Date: 2003/08/08 23:07:50 UTC

OID 1.3.6.1.4.1.14147.1.5.2

1.3. Community and Applicability

1.3.1. Certification Authorities

The Fermilab Service CA does not issue certificates to CAs or people.

1.3.2. Registration Authorities

The Fermilab Computer Security Team operates the Service CA without involving others as Registration Authorities.

1.3.3. End Entities

The Service CA issues certificates to services which operate on Fermilab and affiliated computers. Services are either a generic ‘‘host’’ service associated with a specific computer or a more specific service offered on a single computer or a cluster. Web services traditionally have no service name prefixed to their DNS name.

The keys certified by the Service CA are valid for Digital Signature and Key Encipherment. Its certificates are intended for use with Grid and Web applications.

1.4. Contact Details

The Service CA is extablished, maintained and operated by the Fermilab Computer Security Team. The contact person for this document is the Fermilab Computer Security Coordinator.

Matt Crawford
Fermilab MS-369
PO Box 500
Batavia IL 60510
USA

Phone: +1 630 840 3461
Fax: +1 630 840 6345
Email: nightwatch@fnal.gov

2. GENERAL PROVISIONS

2.1. Obligations

2.1.1. CA Obligations

The Service CA will

- Accept service certificate requests and revocation requests from identified managers or maintainers of Fermilab computers or applications (including instances of such applications on computers away from Fermilab’s physical site), and will notify such requesters of issued and revoked certificates.

- Publish CRLs in a timely manner and in well-known locations.

- Protect and, when necessary or prudent, replace CA private keys.

2.1.2. RA Obligations

No RAs are involved.

2.1.3. Subscriber Obligations

Subscribers must

* Make only accurate representations in requests for certificates.

* Exercise all reasonable care in protecting the private keys corresponding to their certificates, including but not limited to avoiding storage on a networked file system or other transmission over a network.

* Ensure that the private keys corresponding to their issued service certificates are stored in a manner that minimizes the risk of exposure.

* Observe restrictions on private key and certificate use.

* Promptly notify the CA operators of any incident involving a possible exposure of a private key.

2.1.4. Relying Party Obligations

Relying parties must

* Be cognizant of the provisions of this document.

* Verify any self-signed certificates to their own satisfaction.

* Accept responsibility for checking any relevant CRLs before accepting the validity of a certificate.

* Observe restrictions on private key and certificate use.

2.1.5. Repository Obligations

Certificate and Revocation information is maintained on-line with an intended availability of 100%, but the repository is operated on a best-effort basis.

2.2. Liability

The Fermilab Service CA is operated substantially in accordance with Fermilab's own risk analysis. No liability, explicit or implicit, is accepted.

The Fermilab Service CA and its agents make no guarantee about the security or suitability of a service that is identified by a Fermilab certificate. The certification service is run with a reasonable level of security, but it is provided on a best effort only basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.

The Fermilab Service CA denies any financial or other kind of responsibility for damages or impairments resulting from its operation.

2.3. Financial Responsibility

No financial responsibility is accepted.

2.4. Interpretation and Enforcement

This policy is subordinate to all applicable U.S. government laws, as well as Department of Energy (DOE) orders.

2.5. Fees

No fees are charged.

2.6. Publication and Repositories

2.6.1. Publication of CA information

The Fermilab Service CA will operate an online repository that contains

- Fermilab CA certificates.
- A Certificate Revocation List.
- A copy of this policy.
- Other information deemed relevant to the Fermilab PKI.

2.6.2. Frequency of Publication

- CA certificates will be published in the repository as soon as they are issued.
- CRLs will be published as soon as they are updated, or monthly if there are no changes.
- Fermilab PKI documents will be published in the repository as they are approved.

2.6.3. Access Controls

The CA publication repository is always available, outside of maintenance times and unforeseen failures. No restrictions are imposed on the accessibility of published information.

2.6.4. Repository Location

http://computing.fnal.gov/security/pki/

2.7. Compliance Audit

The Fermilab Service CA will be included in Fermilab's regular computer security self-assessment and peer review process but will not be specifically audited by an outside party. Certifying, cross-certifying, and relying organizations may request a review of Fermilab PKI operation.

2.8. Confidentiality Policy

The Fermilab Service CA considers the contents of CRLs and certificates to be public information. The Fermilab Service CA does not obtain or store copies of such private information about individuals.

2.9. Intellectual Property Rights

The Fermilab Service CA asserts no ownership rights in certificates issued to services. No claims are made regarding documents produced by the CA other than as specified in Fermilab's operating contract with the U.S. Department of Energy. Acknowledgment is hereby given to the DOE Science Grid and to the CERN Certification Authority for inspiration of parts of this document.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

3.1.1. Types of Names

All subject distinguished names in certificates issued by the Fermilab PKI begin with ‘‘DC=gov, DC=fnal, O=Fermilab.’’ The next component may be either

OU=Services

for a typical service. An optional second OU component may follow, naming the division, section, or experiment responsible for the service. A CN component will follow the OU or OUs, naming the service and the fully qualified domain name (FQDN) at which the service can be contacted, separated by a slash character. When the service is https, the service name and separator will be absent, and there may be multiple FQDNs and possibly a regular expression expressed as a sequence of CN components.

OU=Automata

for a certificate identifying an automated process acting at the instigation of a service or host, but not on behalf of a specific user. Two or three of the following components complete the Subject name: an OU component containing the division, section, or experiment responsible for the process; a USERID component containing the Fermilab computer account assigned to the activity; a CN containing the fully qualified domain name of the host on which the corresponding private key resides.

3.1.2. Name Meanings

If the subject name contains a USERID, that component has no significance outside Fermilab. If a CN component is present, it includes the fully qualified DNS name of the service, which is usually that of the host supporting the service. The structure of a service’s CN is designed to support SSL/TLS or GSI services.

3.1.3. Name Interpretation

The subject DN of service certificates will contain a component with OU=Services or OU=Automata. The former denotes processes usually intended to be the responder in a service request, the latter, an initiator.

3.1.4. Name Uniqueness

Each subject name certified by the Service CA will be unique.

3.1.5. Name Disputes

The CA will resolve disputes as it sees fit.

3.1.6. Method to Prove Possession of Private Key

Certificate Signing Requests must be signed with the private key corresponding to the public key in the request. The signature will be checked before the certificate is issued.

3.1.7. Authentication of Individual Identity

Requests for service certificates must come from a valid Fermilab user and will be checked against registered system administrator information.

3.2. Rekeying

Subsequent certificate requests are subject to the same validation as initial requests.

3.3. Revocation Requests

Requests for revocation of service certificates from Fermilab computer security personnel and from administrators of the systems hosting the services in question will be honored.

4. OPERATIONAL REQUIREMENTS

4.1. Certificate Application

System and application administrators may request service certificates by emailing a certificate signing request conforming to Fermilab PKI requirements.

4.2. Certificate Issuance

Service certificates are returned to the requesting system or application administrator through email.

4.3. Certificate Acceptance

No stipulation.

4.4. Certificate Suspension and Revocation

Certificates will not be suspended.

4.4.1. Circumstances for Revocation

Service certificates may be revoked in any of the following circumstances.

- The private key is suspected or reliably reported to be lost or exposed.
- The information in the certificate is believed to be, or to have become, inaccurate.
- The certificate is reliably reported to be no longer needed.

4.4.2. Requesting Revocation

System or application administrators may request revocation of a service certificate, as can Fermilab computer security personnel.

4.4.3. Verifying Revocation Requests.

A revocation request signed with the private key of the affected certificate is always valid. Other revocation requests will be examined by the Fermilab Computer Security Team and appropriate action will be taken.

4.4.4. CRL Issuance Frequency

CRLs for the Service and Top-Level CAs will be issued upon any change in their contents, or monthly if there are no changes. New CRLs will be published at least seven days before the expiration of the last previously-published CRL.

4.4.5. Online Revocation/Status Checking Availability

The most recent CRL will be available online.

4.4.6. Revocation/Status Checking Requirements

Relying parties are advised to obtain and consult a valid CRL.

4.5. Security Audit Procedures

No stipulation.

4.6. Records Archival

No stipulation.

4.7. Key Changeover

The community of known relying parties will be notified of any new CA public key and it may then be obtained in the same manner as the previous CA certificates.

4.8. Compromise and Disaster Recovery

If the Service CA is corrupted or compromised its certificate will be revoked by the Top-Level CA and a new key generated. This information will be disseminated to subscribers and known relying parties.

4.9. CA Termination

When the Fermilab PKI terminates its services the fact will be advertised, particularly to users and known relying parties. The CA certificate will be revoked and the final CRL will be made widely available, including at the repository location defined in section 2.6.4.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1. Physical Security Controls

The Service CA is hosted on a server located in a keycard-controlled computer room where all occupants are required to wear Fermilab ID badges or be accompanied. It is not connected to a data network.

5.2. Procedural Controls

No Stipulation.

5.3. Personnel Security Controls

All persons with access to a CA's secret key, or the activation data for it, will be full-time Fermilab employees in the computer security organization.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Private Key Generation

The Fermilab Service CA does not generate any private keys but its own. The CA keys are generated on the system where they will be used, and the Certificate Signing Requests are transported to a superior CA on removable media.

System and service administrators will generate private keys for their services, on the service hosts themselves if possible.

6.1.2. Private Key Delivery to Entity

Not necessary.

6.1.3. Public Key Delivery to Certificate Issuer

Service public keys are delivered, signed, by email and verified by personal contact.

6.1.4. CA Public Key Delivery to Users

The public key of the Service CA may be verified through the superior CA's public key or by out-of-band contact with the CA operator.

6.1.5. Key Sizes

Public RSA keys shorter than 1024 bits will not be certified.

6.1.6. Key Usage

The Service CA does not enforce key usage restrictions by any means beyond the X.509v3 extensions in the certificates it issues. Those extensions will mark the associated keys as valid for Digital Signature and Key Encipherment.

Certificates issued by the Service CA are not recommended to be used for non-repudiation, data confidentiality or message integrity.

6.2. Private Key Protection

6.2.1. Key Generation Modules

No stipulation

6.2.2. Multiperson Control

Not used.

6.2.3. Key Escrow

Not Supported.

6.2.4. Private Key Archival and Backup

No stipulation.

6.2.5. CA Private Key Activation

The Service CA key is activated by logging into the CA host system and entering the passphrase of 15 characters or more. The private key is then available only until signing operations are complete.

6.3. Other Aspects of Key Pair Management

End entity keys are not archived by the Fermilab PKI. CA private keys are not archived beyond their validity period. The Service CA key lifetime is two and one-half years.

6.4. Activation Data

The Service CA private key is encrypted under a pass phrase.

6.5. Computer Security Controls

The Service CA is hosted on a computer system which is used only for Fermilab PKI operations, is not connected to a data network, and which requires physical presence for access.

6.6. Life Cycle Security Controls

No Stipulation

6.7. Network Security Controls

The Service CA is not connected to a data network.

6.8. Cryptographic Module Engineering Controls

No Stipulation

7. CERTIFICATE AND CRL PROFILES

7.1. Certificate Profiles

7.1.1. Service Certificates

```
Subject:
  DC=gov/DC=fnal/O=Fermilab/OU=Services/CN=<svcname>/<f.q.d.n>
Issuer:
  DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=Service CA
Validity:
   (up to a 13 month period)
Subject Public Key Info:
  (provided by applicant - recommend RSA, 2048 bits)
X509v3 Extensions
  X509v3 Basic Constraints: critical
     CA:false
  Netscape Cert Type:
     SSL Client, SSL Server, Object Signing
  X509v3 Key Usage (critical):
     Digital Signature, Key Encipherment
  Netscape Comment:
      "Service certificate issued by Fermilab CA"
    Netscape SSL Server Name:
      <f.q.d.n>
    X509v3 Subject Key Identifier
     ...
    X509v3 Authority Key Identifier
     ...
    X509v3 Subject Alternative Name:
      DNSName:<f.q.d.n>
      Email:(responsible party)
    X509v3 CRL Distribution Points:
     URI:http://computing.fnal.gov/security/pki/fnal-root-crl.crl
    Netscape CA Policy URL:
      http://computing.fnal.gov/security/pki/FNAL-SERVICE-CP-CPS.pdf
```

For a web server, the <svcname> and slash character will be omitted from the Subject Common Name. For a Grid service, the <svcname> will be ‘‘host’’ or some more specific service.

7.1.2. Certificate Policy Object Identifier

iso(1) org(3) dod(6) iana(1) private(4) enterprises(1) Fermilab(14147) security(1) documents(5) serviceCPS(2).

7.2. CRL Profile

The CRL is in version 1 format.

8. Specification Administration

8.1. Specification Change Procedures

Peer PKI operators will be notified of changes.

8.2. Publication

The policy will be available at http://computing.fnal.gov/security/docs/.

8.2.1. CPS Approval Procedures

The Fermilab computer security team approves practices compliant with this policy and statement.